This listing of claims replaces all prior versions, and listings of claims in the instant application:

Listing of Claims:

1.   (Currently Amended)   A method for controlling user access to distributed resources on a data communications network, the method comprising:

receiving, by a resource server peer group, a resource request <u>for a resource stored on said resource server peer group</u>, said resource request including<u>, at time of receipt of said resource request itself, a request for said resource and</u> a rights key credential, said rights key credential comprising:

at least one key to provide access to a resource on said data communications network <u>so that said at least one key is included in said resource request</u>; and

a resource identifier <u>included in said resource request</u>, said resource identifier comprising a resource server peer group ID and a randomized user ID, said resource server peer group ID identifying said resource server peer group, said resource server peer group comprising at least one server that maintains a mapping between said randomized user ID and said at least one key, wherein said randomized user ID is associated with an identity of a user thereby protecting said identity; and

providing ~~access to~~ said resource by said resource server peer group when said <u>resource server peer group matches said</u> at least one key ~~matches~~ <u>with</u> an identifier in a set of identifiers associated with said resource <u>so that said receiving, said providing and said matching are performed on said resource server peer group without</u>

accessing another server outside said resource server peer group.

2.   (Currently Amended)   A method for controlling user access to distributed resources on a data communications network, the method comprising:

receiving, by a resource server peer group, a resource request for a resource stored on said resource server peer group, said resource request including, at time of receipt of said resource request itself, a request for said resource and a rights key credential, said rights key credential comprising:

at least one key, each of said at least one key providing access to at least one resource on said data communications network so that said at least one key is included in said resource request, each of said at least one resource stored on a separate secure device; and

a resource identifier included in said resource request, said resource identifier comprising a resource server peer group ID and a randomized user ID, said resource server peer group ID identifying said resource server peer group, said resource server peer group comprising at least one server that maintains a mapping between said randomized user ID and said at least one key, wherein said randomized user ID is associated with an identity of a user thereby protecting said identity; and

providing access to said resource by said resource server peer group when said resource server peer group matches said at least one key matches with an identifier in a set of identifiers associated with said resource so that said receiving, said providing and said matching are performed on said resource server peer group without

accessing another server outside said resource server peer
group.

3.   (Currently Amended)   A program storage device readable
by a machine, embodying a program of instructions executable by
the machine to perform a method for controlling user access to
distributed resources on a data communications network, the
method comprising:

receiving, by a resource server peer group, a
resource request for a resource stored on said resource
server peer group, said resource request including, at
time of receipt of said resource request itself, a request
for said resource and a rights key credential, said rights
key credential comprising:

at least one key to provide access to a resource
on said data communications network so that said at
least one key is included in said resource request;
and

a resource identifier included in said resource
request, said resource identifier comprising a
resource server peer group ID and a randomized user
ID, said resource server peer group ID identifying
said resource server peer group, said resource server
peer group comprising at least one server that
maintains a mapping between said randomized user ID
and said at least one key, wherein said randomized
user ID is associated with an identity of a user
thereby protecting said identity; and

providing access to said resource by said resource
server peer group when said resource server peer group
matches said at least one key matches with an identifier
in a set of identifiers associated with said resource so
that said receiving, said providing and said matching are
performed on said resource server peer group without

accessing another server outside said resource server peer group.

4.   (Currently Amended)   A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for controlling user access to distributed resources on a data communications network, the method comprising:

receiving, by a resource server peer group, a resource request for a resource stored on said resource server peer group, said resource request including, at time of receipt of said resource request itself, a request for said resource and a rights key credential, said rights key credential comprising:

at least one key, each of said at least one key providing access to at least one resource on said data communications network so that said at least one key is included in said resource request, each of said at least one resource stored on a separate secure device; and

a resource identifier included in said resource request, said resource identifier comprising a resource server peer group ID and a randomized user ID, said resource server peer group ID identifying said resource server peer group, said resource server peer group comprising at least one server that maintains a mapping between said randomized user ID and said at least one key, wherein said randomized user ID is associated with an identity of a user thereby protecting said identity; and

providing access to said resource by said resource server peer group when said resource server peer group matches said at least one key matches with an identifier in a set of identifiers associated with said resource so that said receiving, said providing and said matching are

performed on said resource server peer group without accessing another server outside said resource server peer group.

5.   (Currently Amended)   An apparatus for controlling user access to distributed resources on a data communications network, the apparatus comprising:

means for receiving, by a resource server peer group, a resource request for a resource stored on said resource server peer group, said resource request including, at time of receipt of said resource request itself, a request for said resource and a rights key credential, said rights key credential comprising:

at least one key to provide access to a resource on said data communications network so that said at least one key is included in said resource request; and

a resource identifier included in said resource request, said resource identifier comprising a resource server peer group ID and a randomized user ID, said resource server peer group ID identifying said resource server peer group, said resource server peer group comprising at least one server that maintains a mapping between said randomized user ID and said at least one key, wherein said randomized user ID is associated with an identity of a user thereby protecting said identity; and

means for providing ~~access to~~ said resource by said resource server peer group when said resource server peer group matches said at least one key ~~matches~~ with an identifier in a set of identifiers associated with said resource so that said receiving, said providing and said matching are performed on said resource server peer group without accessing another server outside said resource server peer group.

6.   (Currently Amended)   An apparatus for controlling user access to distributed resources on a data communications network, the apparatus comprising:

means for receiving, by a resource server peer group, a resource request <u>for a resource stored on said resource server peer group</u>, said resource request including<u>, at time of receipt of said resource request itself, a request for said resource and</u> a rights key credential, said rights key credential comprising:

at least one key, each of said at least one key providing access to at least one resource on said data communications network <u>so that said at least one key is included in said resource request</u>, each of said at least one resource stored on a separate secure device; and

a resource identifier <u>included in said resource request</u>, said resource identifier comprising a resource server peer group ID and a randomized user ID, said resource server peer group ID identifying said resource server peer group, said resource server peer group comprising at least one server that maintains a mapping between said randomized user ID and said at least one key, wherein said randomized user ID is associated with an identity of a user thereby protecting said identity; and

means for providing ~~access to~~ said resource by said resource server peer group when said <u>resource server peer group</u> matches said at least one key ~~matches~~ with an identifier in a set of identifiers associated with said resource <u>so that said receiving, said providing and said matching are performed on said resource server peer group without accessing another server outside said resource server peer group</u>.

7.   (Previously Presented)   The method of Claim 1 wherein said rights key credential further comprises a nested credential referring to at least one credential relating to a resource delivery mechanism.

8.   (Currently Amended)   The method of Claim 8 wherein said providing said resource~~access~~ further comprises using said resource delivery mechanism.

9.   (Previously Presented)   The method of Claim 2 wherein said rights key credential further comprises a nested credential referring to at least one credential relating to a resource delivery mechanism.

10.   (Currently Amended)   The method of Claim 9 wherein said providing said resource~~access~~ further comprises using said resource delivery mechanism.